UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,916	06/24/2003	Jari T. Malinen	50072.64US01/NC28794	4349

38879 7590 01/25/2005

DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257

EXAMINER	
MATTIS, JASON E	

ART UNIT	PAPER NUMBER
2665	

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/603,916	MALINEN ET AL.	
	Examiner	Art Unit	
	Jason E Mattis	2665	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5/3/04.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

Page 11 line 13 of the specification incorrectly refers to "the encrypted VPN packet" as item "211". The correct corresponding item number should be "221" as shown in Figure 1C.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 7-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

More specifically, line 3 of claim 7, states, "the HA coupled to the router". Since both a "first router" and a "second router" are described in claim 7, it is unclear which router "the router" in line 3 of claim 7 is referring to.

Claim Objections

4. Claim 19 is objected to because of the following informalities:

Lines 3-4 of claim 19 state, "located within the secure network to monitor data directed to the mobile node". Since there is no prior mention of a secure network or a0 mobile node, it is unclear what specific mobile node is being referred to. It is recommended that "located within the secure network to monitor data directed to the mobile node" be changed to "located within a secure network to monitor data directed to a mobile node".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 7-8, 10, and 15-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Adrangi et al. (U.S. Application 10/323486).

With respect to claim 1, Adrangi et al. discloses a system for providing secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components **(See the abstract of Adrangi et al. for reference to a system providing secure mobile roaming using distributed components)**. Adrangi et al. also discloses a mobile node belonging to a home network located within a secure network with the mobile node having a network interface configured to communicate with other nodes **(See page 2 paragraphs 20-22 and Figure 3 of Adrangi et al. for reference to a mobile node 140 having an interface to communicate with other nodes belonging to corporate intranet 100, which is a home network for mobile node 140 and is also a secure network)**. Adrangi et al. further discloses a router configured to forward packets between networks **(See page 3 paragraph 28, page 4 paragraph 32, and Figure 3 of Adrangi et al. for reference to home agents 305 and 300 both acting as routers to route packets between networks)**. Adrangi et al. also discloses a Proxy Home Agent connected to the home network and located within the secure network that is configured to provide a portion of the Mobile IP Home Agent functionality **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within the corporate intranet 100)**. Adrangi et al. further discloses a Home Agent located outside of the secure network that is configured to provide another portion of the Mobile IP Home Agent functionality **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate**

intranet 100). Adrangi et al. also discloses a VPN gateway coupled to the router and the secure network and configured to work in conjunction with the PHA and the HA **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to VPN gateway 225 coupled to home agent 305, which is a router, and coupled to the corporate intranet 100 to work with the home agents 300 and 305)**.

With respect to claim 2, Adrangi et al. discloses that the VPN gateway and the HA are located within a single device within a DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305 and VPN gateway 225 being located on a single processing device within a corporate DMZ 210)**.

With respect to claim 3, Adrangi et al. discloses a firewall coupled to the secure network and the VPN gateway **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15 and outer firewall 20 being couple to the corporate intranet 100 and the VPN gateway 225)**.

With respect to claim 4, Adrangi et al. discloses that the HA is a separate devices from the VPN gateway **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to the home agent 305 being implemented on an independent processing device within corporate DMZ 210, meaning the home agent 305 is a separate device from VPN gateway 225)**.

With respect to claim 7, Adrangi et al. discloses a DMZ comprising a first router coupled to a second router that is coupled to the firewall with the VPN gateway couple to the first router and the firewall and the HA coupled to the router **(See page 2 paragraph 20 of Adrangi et al. for reference to VPN gateway 225, which acts as a**

first router by routing packets, for reference to the VPN gateway 225 being coupled to the home agent 305, which acts as a second router by routing packets, and for reference to the VPN gateway 225 and the home agent 305 being coupled to firewalls 15 and 20).

With respect to claim 8, Adrangi et al. discloses that packets from the MN destined towards nodes inside the secure network first go to the HA and then to the VPN gateway that is configured to forward the packets through the firewall to the secure network **(See page 3 paragraph 27 and Figure 4 of Adrangi et al. for reference to packets sent from MN 140 to CN 310, which is a node inside of the corporate network 100, being first sent to home agent 305 and then to VPN gateway 225, which sends the packets through the firewall to CN 310).**

With respect to claim 10, Adrangi et al. discloses that the router is directly connected to a firewall and the VPN gateway and the HA are connected to a different interface of the router and the firewall **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to VPN gateway 225 being connected to an inner firewall 15 and an outer firewall 20 and for reference to the VPN gateway 225 and the home agent 305 being separate devices meaning that their connections to the firewalls 15 and 20 are through separate interfaces).**

With respect to claim 15, Adrangi et al. discloses a method for secure communication **(See the abstract of Adrangi et al. for reference to a method providing secure mobile roaming).** Adrangi et al. also discloses a mobile node associated with a home network in a secure network and a corresponding node **(See**

page 2 paragraphs 20-22 and Figure 3 of Adrangi et al. for reference to a mobile node 140 having an interface to communicate with other nodes, including CN 310, belonging to corporate intranet 100, which is a home network for mobile node 140 and is also a secure network). Adrangi et al. further discloses establishing a Proxy Home Agent located within the secure network to monitor data directed to the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within the corporate intranet 100)**. Adrangi et al. also discloses establishing a Home Agent configured to create a security association with the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate intranet 100)**. Adrangi et al. further discloses collecting data directed to the mobile node **(See page 2 paragraph 20 to page 3 paragraph 25 of Adrangi et al. for reference to both home agent 300 and home agent 305 being used to collect and route data directed to the mobile node 140)**. Adrangi et al. also discloses packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data and tunneling the VPN packaged data to a current address of the mobile node **(See page 3 paragraphs 26-28 and Figure 4 of Adrangi et al. for reference to using a VPN gateway 225 to package data in a secure VPN tunnel to an internal address of the mobile node 140 and tunneling the data to a care of address of the mobile node 140)**.

With respect to claim 16, Adrangi et al. discloses that the VPN secure tunnel follows the IP security protocol **(See page 2 paragraph 22 of Adrangi et al. for reference to using IPSec protocol)**.

With respect to claim 17, Adrangi et al. discloses that the tunneling of the VPN packaged data to the external mobile node occurs according to the IP mobility protocol **(See page 1 paragraph 3 of Adrangi et al. for reference to using mobile IP standards)**.

With respect to claim 18, Adrangi et al. discloses packaging the collected data in an IP-in-IP tunnel and sending it to a VPN device for VPN encryption and tunneling the VPN packaged data to the current address of the mobile node **(See page 4 paragraph 29 and Figure 6 of Adrangi et al. for reference to packaging the data in an IP-in-IP tunnel and sending it to a VPN gateway 225 for VPN encryption before sending the packet to the care of address of the mobile node)**.

With respect to claim 19, Adrangi et al. discloses a system for secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components **(See the abstract of Adrangi et al. for reference to a system providing secure mobile roaming using distributed components)**. Adrangi et al. also discloses a means for establishing a Proxy Home Agent located within the secure network to monitor data directed to the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 300, which is a Proxy Home Agent providing Mobile IP Home Agent functionality, located within corporate intranet 100, which is a secure network)**. Adrangi et al. further discloses a means for

establishing a Home Agent configured to create a security association with the mobile node **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to home agent 305, which provides Mobile IP Home Agent functionality, located outside the corporate intranet 100)**. Adrangi et al. also discloses a means for collecting data directed to the mobile node **(See page 2 paragraph 20 to page 3 paragraph 25 of Adrangi et al. for reference to both home agent 300 and home agent 305 being used to collect and route data directed to the mobile node 140)**. Adrangi et al. further discloses a means for packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data and a means for tunneling the VPN packaged data to a current address of the mobile node **(See page 3 paragraphs 26-28 and Figure 4 of Adrangi et al. for reference to using a VPN gateway 225 to package data in a secure VPN tunnel to an internal address of the mobile node 140 and tunneling the data to a care of address of the mobile node 140)**. Adrangi et al. also discloses a means for the Home Agent to communicate to the PHA that the mobile node has either moved outside its home network or has come back to its home network **(See pages 2-3 paragraphs 20-25 of Adrangi et al. for reference to the home agents 300 and 305 updating the current location of the mobile node 140 by storing a current care of address of the mobile node that indicates the location of the node)**. Adrangi et al. further discloses a means for enabling the PHA to create and remove a proxy ARP entry for a permanent address associated with the mobile node **(See page 3 paragraph 25 of Adrangi et al. for reference to home agent 300 creating and removing care of address entries,**

which are proxy ARP entries for a permanent address associated with the mobile node 140).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 5, 9, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adrangi et al. in view of Liu et al. (U.S. Application 10/145378).

With respect to claim 5, Adrangi et al. discloses a DMZ located outside the secure network wherein the VPN gateway and the HA reside in the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to corporate DMZ 210 that is located outside the secure network and includes the VPN gateway 225 and home agent 305)**. Adrangi et al. also discloses a first firewall between the secure network and the DMZ and a second firewall between the DMZ and an external network **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15, which is a first firewall located between the corporate intranet 100 and the DMZ 210, and for reference to outer firewall 20, which is a second firewall located between the DMZ 210 and an external network 205)**. Adrangi et al. also

discloses that the mobile node has a permanent address in a known range **(See page 1 paragraph 12 of Adrangi et al. for reference to a mobile node 140 having a permanent address that all data directed towards the mobile node is addressed to and for reference to a home agent intercepting and rerouting data to a care of address of the mobile node when the mobile node has exited its home network)**. Adrangi et al. does not specifically disclose that the firewall is configured to deny communications from the external network with a source address in a known range.

With respect to claim 9, Adrangi et al. does not disclose a firewall dropping packets having a source address in a known range.

With respect to claim 14, Adrangi et al. discloses a firewall coupled to the secure network and the VPN gateway **(See page 2 paragraph 20 of Adrangi et al. for reference to inner firewall 15 coupled to both the corporate intranet 100 and the VPN gateway 225)**. Adrangi et al. does not disclose dropping packets having a source address in a known range.

With respect to claims 5, 9, and 14, Liu et al., in the field of communications, discloses a firewall dropping packets having a source address in a known range **(See page 2 paragraph 19 of Liu et al. for reference to maintaining an ALC table 104 that is used to store address and ranges of address and a field indicating that the address or range of address should be dropped by a firewall)**. Using a firewall that drops packets having a source address in a known range has the advantage of allowing better control of the packets that are allowed to enter a secure network to protect against malicious packets.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Liu et al., to combine using a firewall that drops packets having a source address in a known range, as suggested by Liu et al., with the system and method of Adrangi et al., with the motivation being to allow better control of the packets that are allowed to enter a secure network to protect against malicious packets.

9. Claims 6 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adrangi et al. in view of Liu et al. as applied to claims 5, 9, and 14 above, and further in view of Mikkonen (U.S. Application 10/185714).

With respect to claim 6, Adrangi et al. discloses a DMZ located outside the secure network wherein the VPN gateway and the HA reside in the DMZ **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to corporate DMZ 210 that is located outside the secure network and includes the VPN gateway 225 and home agent 305)**. Adrangi et al. also discloses a first firewall between the secure network and the DMZ and a second firewall between the DMZ and an external network **(See page 2 paragraph 20 and Figure 3 of Adrangi et al. for reference to inner firewall 15, which is a first firewall located between the corporate intranet 100 and the DMZ 210, and for reference to outer firewall 20, which is a second firewall located between the DMZ 210 and an external network 205)**. Adrangi et al. further discloses that the mobile node has a permanent address in a known range **(See page 1 paragraph 12 of Adrangi et al. for reference to a mobile node 140 having a**

permanent address that all data directed towards the mobile node is addressed to and for reference to a home agent intercepting and rerouting data to a care of address of the mobile node when the mobile node has exited its home network). Liu et al. discloses a firewall dropping packets having a source address in a known range **(See page 2 paragraph 19 of Liu et al. for reference to maintaining an ALC table 104 that is used to store address and ranges of address and a field indicating that the address or range of address should be dropped by a firewall)**. The combination of Liu et al. and Adrangi et al. does not disclose that the VPN gateway has a direct connection to an internal interface of the first firewall.

With respect to claim 11, Liu et al. discloses a firewall dropping packets having a source address in a known range **(See page 2 paragraph 19 of Liu et al. for reference to maintaining an ALC table 104 that is used to store address and ranges of address and a field indicating that the address or range of address should be dropped by a firewall)**. The combination of Liu et al. and Adrangi et al. does not disclose that the VPN gateway has a direct connection to an internal interface of the first firewall.

With respect to claims 6 and 11, Mikkonen, in the field of communications, discloses a firewall with an internal interface to a VPN gateway **(See page 2 paragraph 18 of Mikkonen for reference to a firewall 100 that also is used to operate as a VPN gateway meaning that since the firewall and gateway functions are performed in the same device, that they must have an internal interface with each other)**. Using a firewall with an internal connection to a VPN gateway has the

advantage of allowing the operation of the firewall and VPN gateway to be better integrated so that secure packets received by the VPN gateway can be better filtered by the firewall.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Mikkonen, to combine using a firewall with an internal interface to a VPN gateway, as suggested by Mikkonen, with the system and method of Adrangi et al. and Liu et al., with the motivation being to allow the operation of the firewall and VPN gateway to be better integrated so that secure packets received by the VPN gateway can be better filtered by the firewall.

With respect to claim 12, Liu et al. discloses forwarding and decrypting packets, or otherwise dropping packets, according to a security association that exists **(See page 2 paragraph 19 of Liu et al. for reference to using a table 104 to decide which packets to forward and which packets to drop according to a security payload index)**.

With respect to claim 13, Adrangi et al. discloses that packets from the MN destined towards nodes inside the secure network first go to the HA and then to the VPN gateway that is configured to forward the packets through the firewall to the secure network **(See page 3 paragraph 27 and Figure 4 of Adrangi et al. for reference to packets sent from MN 140 to CN 310, which is a node inside of the corporate network 100, being first sent to home agent 305 and then to VPN gateway 225, which sends the packets through the firewall to CN 310)**.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Liu et al. (U.S. Application 10/325657) discloses a system and method for integrating mobile networking with security-based VPNs.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason E Mattis whose telephone number is (571) 272-3154. The examiner can normally be reached on M-F 8AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jem

HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600